

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:

ERLINGSSON *et al.*

Application No.: 10/627,270

Filed: July 25, 2003

**For: Systems and Methods for
Transparent Configuration
Authentication of Networked
Devices**

Confirmation No.: 7588

Art Unit: 2439

Examiner: Homayounmehr, Farid

Atty. Docket: 2525.0750001

**Brief on Appeal to the Board of Patent Appeals
and Interferences Under 37 C.F.R § 41.37**

Mail Stop Appeal Briefs-Patents

Commissioner for Patents
PO Box 1450
Alexandria, VA 22313-1450

Sir:

A Notice of Appeal from the final rejection of claims 1-25 for the above-captioned U.S. Patent Application was filed on March 9, 2009 appealing the decision of the Examiner in the Final Office Action mailed December 9, 2008 ("Office Action"), maintaining the rejection of claims 1-25.

In support of the Notice of Appeal, Appellants hereby file an appeal brief as required under 37 C.F.R. § 41.37(a)(1). Appellants have also filed herewith the fee for filing a brief in support of an appeal as set forth in 37 C.F.R. § 41.37(a)(2).

The Commissioner is hereby authorized to charge any fee deficiency, or credit any overpayment, to Deposit Account No. 19-0036.

TABLE OF CONTENTS

I.	Real Party in Interest (37 C.F.R. § 41.37(c)(1)(i))	3
II.	Related Appeals and Interferences (37 C.F.R. § 41.37(c)(1)(ii))	3
III.	Status of the Claims (37 C.F.R. § 41.37(c)(1)(iii)).....	3
IV.	Status of Amendments (37 C.F.R. § 41.37(c)(1)(iv)).....	3
V.	Summary of Claimed Subject Matter (37 C.F.R. § 41.37(c)(1)(v))	4
VI.	Grounds of Rejection to be Reviewed on Appeal (37 C.F.R. § 41.37(c)(1)(vi))	5
VII.	Argument (37 C.F.R. § 41.37(c)(1)(vii)).....	6
A.	Claims 1-7, 10-17, and 20-25 are patentable over Moskowitz and Shur	6
1.	Summary of the Examiner's Obviousness Rejection	6
2.	Summary of Cited References	7
(i)	Moskowitz	7
(ii)	Shur.....	8
3.	Claims 1-7, 10-17, and 20-25 are not obvious over Moskowitz and Shur.....	9
(i)	The Combination of Moskowitz and Shur does not Teach or Suggest Each and Every Feature of Claim 1	10
(ii)	The Combination of Moskowitz and Shur Renders Moskowitz Unsatisfactory for Its Intended Purpose ...	15
B.	Claims 8, 9, 18, and 19 are patentable over Moskowitz, Shur, and Examiner Official Notice.....	17
VIII.	Conclusion	19
IX.	Claims Appendix	21
X.	Evidence Appendix.....	28
XI.	Related Proceedings Appendix.....	28

I. Real Party in Interest (37 C.F.R. § 41.37(c)(1)(i))

The real party of interest is Google Inc., having its principal place of business at 1600 Amphitheatre Parkway, Mountain View, California, 94043. An assignment assigning all right, title, and interest in and to the patent application from Green Border Technologies, Inc. to Google Inc. was recorded in the U.S. Patent & Trademark Office on October 23, 2007 at Reel 019995, Frame 0713.

II. Related Appeals and Interferences (37 C.F.R. § 41.37(c)(1)(ii))

To the best of knowledge of Appellants, Appellants' legal representative, and assignee, there are no other appeals or interferences which will directly affect or be directly affected or have a bearing on a decision by the Board of Patent Appeals and Interferences ("the Board") in the pending appeal.

III. Status of the Claims (37 C.F.R. § 41.37(c)(1)(iii))

Pending claims 1-25 were finally rejected in an Office Action mailed December 9, 2008. No claim stands allowed. Accordingly, the claims on appeal are claims 1-25. A copy of the claims on appeal can be found in the attached Claims Appendix as required under 37 C.F.R. § 41.37(c)(1)(viii).

IV. Status of Amendments (37 C.F.R. § 41.37(c)(1)(iv))

All amendments have been entered. No amendments have been filed subsequent to the final rejection mailed December 9, 2008.

V. Summary of Claimed Subject Matter (37 C.F.R. § 41.37(c)(1)(v))

The claimed subject matter relates to methods and systems for watermarking at the packet level.

Independent Claim 1

Independent claim 1 is directed to a method for providing secure transmissions across a network which comprises a client device and a server. The method of claim 1 comprises generating a stream of watermark bits at the client device; generating a plurality of watermarks, with each of the plurality of watermarks comprising a respective index number and a respective portion of the stream of watermark bits; and inserting the plurality of watermarks into respective headers of a plurality of outgoing packets. The method of claim 1 further comprises receiving, at the server, the plurality of outgoing packets, and determining if a received packet is valid based on the watermark contained in the header of the received packet. A detailed description of the subject matter contained in independent claim 1 can be found, for example, in paragraphs [008], [039]-[042], and [047]; and in FIGs. 3 and 4 of Appellants' specification.

Independent Claim 12

Independent claim 12 is directed to a system for providing secure transmissions across a network. The system of claim 12 includes a client device and a server. The client device performs the steps of generating a stream of watermark bits; generating a plurality of watermarks, with each of the plurality of watermarks comprising a respective index number and a respective portion of the stream of watermark bits; inserting the plurality of watermarks into respective headers of a

plurality of outgoing packets; and transmitting the outgoing packets to the server. The server performs the steps of receiving the plurality of outgoing packets, and determining if a received packet is valid based on the watermark contained in the header of the received packet. A detailed description of the subject matter contained in independent claim 1 can be found, for example, in paragraphs [008], [024]-[034], [039]-[042], and [047]; and in FIGs. 1-4 of Appellants' specification.

Independent Claim 21

Independent claim 21 is directed to a system for providing secure transmissions across a network from a client device to a server. The system of claim 21 includes means for generating a stream of watermark bits; means for generating a plurality of watermarks, with each of the plurality of watermarks comprising a respective index number and a respective portion of the stream of watermark bits; means for inserting the plurality of watermarks into respective headers of a plurality of outgoing packets; and means for transmitting the outgoing packets to a server. The server is capable of determining if a received packet is valid based on the watermark contained in the header of the received packet. A detailed description of the subject matter contained in independent claim 1 can be found, for example, in paragraphs [008], [024]-[034], [039]-[042], and [047]; and in FIGs. 1-4 of Appellants' specification.

VI. Grounds of Rejection to be Reviewed on Appeal (37 C.F.R. § 41.37(c)(1)(vi))

In the final Office Action mailed December 9, 2008, the Examiner rejected claims 1-7, 10-17, and 20-25 under 35 U.S.C. § 103(a) as allegedly being

unpatentable over U.S. Patent Application Publication No. 2003/0200439 to Moskowitz *et al.* (“Moskowitz”) in view of U.S. Patent No. 6,330,672 to Shur (“Shur”); and claims 8, 9, 18, and 19 under 35 U.S.C. § 103(a) as allegedly being unpatentable over Moskowitz in view of Shur, and further in view of Examiner Official Notice. Claims 22-25 were finally rejected under 35 U.S.C. § 112, first paragraph; however, this rejection has been overcome and withdrawn by the Examiner as indicated in the Advisory Action mailed February 25, 2009.

Accordingly, the grounds of rejection to be reviewed on appeal are:

- A. Rejection of claims 1-7, 10-17, and 20-25 under 35 U.S.C. § 103(a) over Moskowitz and Shur.
- B. Rejection of claims 8, 9, 18, and 19 under 35 U.S.C. § 103 over Moskowitz, Shur, and Examiner Official Notice.

VII. Argument (37 C.F.R. § 41.37(c)(1)(vii))

A. Claims 1-7, 10-17, and 20-25 are patentable over Moskowitz and Shur

1. Summary of the Examiner’s Obviousness Rejection

In the rejection of claim 1, the Examiner alleges that Moskowitz discloses “generating a plurality of watermarks, each of the plurality of watermarks comprising an index number and a portion of the stream of watermark bits.” *See* Office Action, page 6, lines 11-12. The Examiner concedes that Moskowitz “does not explicitly teach each header receiving a respective different watermark.” *See* Office Action, page 7, lines 1-3. However, the Examiner relies on Shur as allegedly teaching “putting different portions of the watermark string in different parts of the data, and

defining an index, which identifies which part of the data stream is affected by the addition or injection of the watermark stream.” *See* Office Action, page 7, lines 9-12.

Accordingly, the Examiner concludes that “it would have been obvious to one skilled in art to combine the teachings of embedding a string of digital watermark bits into different packets of Moskowitz, and indexing the different portions such that the watermark associated with each packet would be detected by the decoder.” *See* Office Action, page 7, lines 13-18. The Examiner attempts to further clarify the combination of Moskowitz and Shur in the Advisory Action mailed February 25, 2009, by noting that “the proposed rejection relies on Moskowitz to put watermarks and indeces (sic) in each packet . . . [and] [i]t is the process of generation of the watermark and the index that is modified based on Shur.” *See* Advisory Action, page 2, lines 46-47. In particular, the Examiner’s rejection seeks to combine Moskowitz and Shur by considering “each time segment [in Shur] . . . simply equavalent (sic) to [the] payload content of each Moskowitz packet,” generating a “watermark and index” for each time segment based on Shur, and inserting the watermark and index in the packet header as suggested by Moskowitz. *See* Advisory Action, page 2, lines 49-51.

2. Summary of Cited References

(i) Moskowitz

Moskowitz is directed to packet watermarking and efficient provisioning of bandwidth. In particular, Moskowitz discloses a method for transmitting streams of data, which includes “generating **a packet watermark** associated with the stream of data” and “combining the packet watermark **with each of the plurality of packets**”

of the data stream. Moskowitz, Abstract. (Emphasis added). Moskowitz expressly discloses that a **single watermark** is generated and used in a packet stream. *See* Moskowitz, paragraph [0035]. Thus, Moskowitz uses the same watermark in each and every packet of a packet stream.

According to Moskowitz, the watermark assigned to a packet stream may be used to “classify [the packet stream] for a particular QoS.” *See* Moskowitz, paragraph [0030], lines 1-3. As such, Moskowitz discloses a watermark having a first portion reserved for a QoS level indicator and a second portion to hold a flow identifier, Watermark Identification (“WID”). *See* Moskowitz, paragraph [0030], lines 11-17. The WID is used to uniquely identify and authenticate **the packet flow** at a receiver. *See* Moskowitz, paragraph [0033]. Moskowitz expressly discloses that a **single WID** is created per packet stream. *See* Moskowitz, paragraph [0035].

(ii) Shur

Shur is directed to watermarking for piracy protection purposes. In particular, Shur’s method includes inserting a **single watermark** into an information signal such that the watermark is distributed throughout the information signal, thereby making the watermark more difficult to locate and remove by a digital pirate. (Emphasis added). *See e.g.*, Shur, column 3, lines 41-52.

According to Shur, portions of a watermark are inserted at different locations of an information signal by replacing respective information content. In particular, the watermark is inserted based on spectral coefficients of contiguous time segments of the information signal. As such, when content in a time segment of the information signal cannot be removed without perceptible quality loss (i.e., the spectral coefficient

of the time segment is higher than a perception threshold function), no portion of the watermark will be inserted in said time segment. *See e.g.*, Shur, col. 6, lines 38-51; col. 7 line 56 - col. 8, line 8.

In distributing a watermark in an information signal, Shur discloses generating “indexed locations” of the information signal. The indexed locations serve to indicate where portions of the watermark are to be injected into the information signal. *See e.g.*, Shur, column 6, lines 46-51.

As described above, Shur’s method operates on information **content**. Therefore, Shur’s method is not concerned with watermarking **a packet stream** for authentication purposes.

3. *Claims 1-7, 10-17, and 20-25 are not obvious over Moskowitz and Shur*

Independent claim 1 recites, among other features:

generating a plurality of watermarks, each of the plurality of watermarks comprising a respective index number and a respective portion of the stream of watermark bits;
inserting the plurality of watermarks into respective headers of a plurality of outgoing packets.

In rejecting claim 1, the Examiner suggests that Moskowitz and Shur can be combined to result in the above recited features of claim 1. In particular, the Examiner alleges that Moskowitz would provide inserting of a watermark and an index number in each packet and that Shur would provide generating a plurality of watermarks and associated respective index numbers. *See* Advisory Action, page 2, lines 26-27 and 46-47. For the reasons provided below, Appellants assert that

Moskowitz and Shur, alone or in combination, do not teach or suggest each and every feature of claim 1. Appellants further assert that the combination of Moskowitz and Shur, as suggested by the Examiner, would render Moskowitz unsatisfactory for its intended purpose.

(i) The Combination of Moskowitz and Shur does not Teach or Suggest Each and Every Feature of Claim 1

Independent claim 1 recites, *inter alia*, “generating **a plurality of watermarks**, each of the plurality of watermarks comprising **a respective index number** and a respective portion of the stream of watermark bits.” (Emphasis added).

Neither Moskowitz nor Shur teaches or suggests generating a plurality of watermarks. Indeed, as described above, Moskowitz discloses using **a single watermark** per packet stream. Shur, on the other hand, discloses distributing a **single watermark** into an information signal at indexed locations of the information signal. Further, since both Moskowitz and Shur use only a single watermark, neither Moskowitz nor Shur teaches or suggests “each of the plurality of watermarks comprising **a respective index number**,” as recited in claim 1. (Emphasis added). Indeed, with a single watermark, an index number to index the watermark would not be needed.

However, the Examiner contends that Shur’s process of distributing a single watermark in an information signal is equivalent to “generating a plurality of watermarks” because allegedly, according to Shur, different portions of the

information signal receive different portions of the watermark. *See* Advisory Action, page 2, lines 4-7. The Examiner further claims that “Moskowitz parag. 31 teaches an index in each watermark.” *See* Advisory Action, page 2, lines 18-19. In addition, the Examiner contends that Shur can be used to modify Moskowitz’s process of generating an index so as to generate “a different watermark and its associated (respective) index” for each packet. *See* Advisory Action, lines 26-27; lines 46-51. For the reasons provided below, Appellants disagree with the Examiner.

First, Appellants assert that Shur does not teach or suggest “generating a plurality of watermarks,” as recited in claim 1. Indeed, Shur only teaches that a **single watermark** is inserted into an information signal. *See e.g.*, Shur, Abstract. Further, nowhere does Shur teach or suggest using more than a single watermark in the information signal. In addition, the Examiner’s allegation that different time segments in Shur receive different portions of the watermark does not change the fact that Shur **generates only a single watermark, not a plurality of watermarks**.

In addition, Appellants assert that Moskowitz modified by Shur, as suggested by the Examiner, does not teach or suggest “each of the plurality of watermarks comprising a respective index number,” as recited in claim 1.

Indeed, as noted above, Moskowitz discloses a watermark having a first portion reserved for a QoS level indicator and a second portion to hold a flow identifier, Watermark Identification (“WID”). *See* Moskowitz, paragraph [0030], lines 11-17. The WID is used to uniquely identify and authenticate **the packet flow** at a receiver. *See* Moskowitz, paragraph [0033]. Moskowitz expressly discloses that a **single WID** is created per packet stream. *See* Moskowitz, paragraph [0035]. Thus,

assuming for the sake of argument that a WID is equivalent to an “index number” as recited in claim 1, then Moskowitz teaches that the same index number is used for each and every packet in the stream.

The Examiner, however, relies on Shur to modify Moskowitz. For this purpose, the Examiner, throughout the rejection, makes numerous references to what the Examiner calls “indices” or “index” of Shur and further suggests that Shur teaches that these alleged “indices” or “index” are part of the watermark or inserted with the watermark. *See e.g.*, Advisory Action, line 25; line 27; line 35; lines 37-38; lines 48-49; and lines 49-50. However, as discussed below, Appellants strongly assert that the Examiner is incorrectly interpreting the function of these alleged “indices” or “index” of Shur.

First, Appellants wish to point out that Shur makes no mention at all of “indices” or an “index” as alleged by the Examiner. Rather, Shur describes “indexed locations.” Further, it is clear that it is these “indexed locations” that the Examiner now refers to as “indices.” *See* Office Action, page 7, lines 4-12.

In addition, Appellants assert that (1) an “indexed location” of Shur is not equivalent to “a respective index number” as recited in claim 1; and (2) even assuming, *arguendo*, that an “indexed location” of Shur can be equivalent to a “respective index number,” the “indexed location” of Shur is not a part of the watermark, as recited in claim 1.

Indeed, as described above, in distributing a watermark in an information signal, Shur discloses generating “indexed locations” of the information signal. The indexed locations **serve to indicate where portions of the watermark are to be**

injected into the information signal. *See e.g.,* Shur, column 6, lines 46-51. However, the “indexed locations” do not serve as respective identifiers of a plurality of watermarks. Furthermore, Shur does not teach or suggest, nor has the Examiner offered any evidence of an alleged teaching by Shur, that the “indexed locations” are **inserted into the information signal as part of the watermark.**

Therefore, Appellants assert that Shur does not teach or suggest generating “indices” or an “index” as alleged by the Examiner. Further, Appellants assert that Shur’s “indexed locations” are not equivalent to “a respective index number,” as recited in claim 1. Accordingly, Appellants conclude that the Examiner’s allegation that Moskowitz’s process of generating an “index” can be modified by Shur’s process so as to generate “a different watermark and its associated (respective) index” for each packet is without technical basis based on the teachings of Shur.

For at least the reasons provided above, Appellants assert that the combination of Moskowitz and Shur does not teach or suggest “generating a plurality of watermarks, each of the plurality of watermarks comprising a respective index number,” as recited in claim 1.

Independent claim 1 further recites, *inter alia*, “inserting the plurality of watermarks into **respective headers** of a plurality of outgoing packets.” (Emphasis added).

The Examiner’s combination of Moskowitz and Shur relies on Moskowitz to insert watermarks generated according to Shur into packet headers. *See e.g.,* Advisory Action, page 2, lines 26-27; *see also* Advisory Action, page 2, lines 49-50. In particular, the Examiner suggests that Shur’s watermarking can be applied to the

payloads of packets of Moskowitz. The resulting “indices” of Shur can then be extracted, the watermarks can be generated, and the watermarks and the “indices” can be inserted into the packet headers. *See* Advisory Action, page 2, lines 34-36. For the reasons below, Appellants assert that such combination as described by the Examiner is technically unfeasible based on the teachings of Moskowitz and Shur, and would not result in the above recited feature of claim 1.

First, assume for the sake of argument that Shur’s watermarking method can be used on the payload of a packet of Moskowitz. The result of such watermarking would be a payload with a watermark **inserted** at different locations **in the payload**. Alternatively, if Shur’s watermarking is applied to an aggregate payload of multiple packets of Moskowitz, then the result would be the aggregate payload with a watermark distributed throughout the **aggregate payload**. Thus, watermarking according to Shur does not result in a watermark inserted **into the header of a packet**.

The Examiner, however, suggests that the watermark and the “indices” can be somehow extracted so that they can be inserted into the headers of packets using Moskowitz. *See* Advisory Action, page 2, line 35. However, such allegation is incorrect based on the teachings of Shur. Indeed, referring to FIG. 1B of Shur, it is clear that once the watermark is injected into the information signal by coefficient quantizer 106, the watermark or portions thereof no longer exist in discrete form so that they can be inserted into packet headers. Rather, as described by Shur, the watermark is distributed throughout the output bitstream of quantizer 106 such that it is “not easily recognizable and locatable.” *See* Shur, column 10, lines 54-62. Further,

the watermark may be extracted only when the information signal is decoded by a decoder. *See e.g.*, Shur, column 11, lines 24-34. In addition, as discussed above, no “indices” are inserted within or with the watermark according to Shur. Thus, no extraction of such “indices” is possible either.

Accordingly, the combination of Moskowitz and Shur, as suggested by the Examiner, would result in watermark bits inserted into **payloads of packets, not into “respective headers” of packets**, as recited in claim 1. Further, the watermark bits would include no “respective index number” as recited in claim 1.

For at least the reasons provided above, Appellants assert that the combination of Moskowitz and Shur does not teach and suggest “inserting the plurality of watermarks into respective headers of a plurality of outgoing packets,” as recited in claim 1.

“All words in a claim must be considered in judging the patentability of that claim against the prior art.” M.P.E.P. § 2143.03. To establish a *prima facie* case of obviousness, “the prior art reference (or references when combined) must teach or suggest all the claim limitations.” M.P.E.P. § 2142. Accordingly, the Examiner has failed to establish a *prima facie* case of obviousness regarding claim 1.

**(ii) *The Combination of Moskowitz and Shur Renders
Moskowitz Unsatisfactory for Its Intended Purpose***

As described above, Moskowitz is directed to packet watermarking and efficient provisioning of bandwidth. As such, Moskowitz discloses a watermark having a QoS portion reserved for a QoS level indicator and a WID (Watermark Identification) portion to hold a flow identifier. *See* Moskowitz, paragraph [0030], lines 11-17.

The QoS portion of the watermark in Moskowitz is used to “classify [the packet stream] for a particular QoS.” *See* Moskowitz, paragraph [0030], lines 1-3. The WID portion of the watermark is used to **uniquely identify** and authenticate **the packet flow** at a receiver. *See* Moskowitz, paragraph [0033]. For these purposes, Moskowitz expressly discloses that **the same watermark should be used in each and every packet of the packet flow**. *See e.g.*, Moskowitz, paragraph [0030], lines 7-9; *see also* Moskowitz, paragraph [0034], lines 5-7; paragraph [0035].

Clearly, therefore, Moskowitz would be rendered unsatisfactory for its intended purpose if either the QoS portion or the WID portion of the watermark is modified from one packet to another in the packet stream. Indeed, if the QoS portion is modified, then different packets of the packet stream would receive different QoS treatment as they are routed through the network. This is clearly not the intended purpose of Moskowitz, which uses the QoS portion of the watermark to classify the entire packet stream’s QoS. Similarly, if the WID portion is modified, then the receiver according to Moskowitz would lose its ability to identify packets of the same stream, thereby rendering Moskowitz unsatisfactory for its intended purpose of identifying a packet stream using its associated WID. “If proposed modification would render the prior art invention being modified unsatisfactory for its intended purpose, then there is no suggestion or motivation to make the proposed modification.” M.P.E.P. § 2143.01(V). Accordingly, a person of ordinary skill in the art would not have combined Moskowitz and Shur.

For at least the reasons provided above, claim 1 is patentable over Moskowitz and Shur. The rejection of claim 1 and of claims 2-7, 10, and 22-23 which depend therefrom must be reversed.

Independent claims 12 and 21 recite similar features as discussed above with respect to claim 1 and are rejected along the same rationale. Therefore, for at least the reasons provided above, claims 12 and 21 are patentable over Moskowitz and Shur. The rejection of claims 12 and 24 and of claims 13-17, 20, and 24-25 which depend therefrom must be reversed.

***B.* Claims 8, 9, 18, and 19 are patentable over Moskowitz, Shur, and Examiner Official Notice**

Claims 8, 9, 18, and 19 depend from one of claims 1 and 12. Accordingly, for at least the reasons provided above with respect to claims 1 and 12, claims 8, 9, 18, and 19 are patentable over Moskowitz and Shur. The Examiner relies on Examiner Official Notice to reject a feature of claim 8 regarding the use of a pivotal index number. However, Examiner Official Notice does not overcome the deficiencies of Moskowitz and Shur as described above. Therefore, for at least the reasons provided above, claims 8, 9, 18, and 19 are patentable over Moskowitz, Shur, and Examiner Official notice. Moreover, claims 8, 9, 18, and 19 are patentable over Moskowitz, Shur, and Examiner Official Notice in view of their own patentable features as further discussed below.

Indeed, in rejecting claim 8, the Examiner alleges that Moskowitz and Shur are directed to the method of claim 5. *See* Office Action, page 10, line 14. The Examiner further alleges that “Moskowitz teaches comparing the packet’s watermark

to the watermarks in a first and second window [and] . . . also teaches recording and using a pivotal index number of representing the index number of the highest-numbered valid watermark received from the transmitting device in paragraphs 32-42.” *See* Office Action, page 11, lines 3-7. In addition, the Examiner takes official notice that “considering the last packet as the pivotal packet, the matching watermarks corresponding to the other packets in the stream will be found sequentially at the preceding locations relative to matching watermark corresponding to the last packet of the stream.” *See* Office Action, page 11, lines 13-16.

Appellants have carefully examined Moskowitz, including paragraphs 32-42 referred to by the Examiner. However, Appellants found no reference in Moskowitz to the alleged teachings by the Examiner. In particular, Moskowitz makes no mention or suggestion of “comparing the watermark . . . to a first and a second window, each of the windows comprising a set of expected watermarks,” or “maintaining . . . a record of a pivotal index number representing the index number of the highest-numbered valid watermark received,” as recited in claim 8.

Appellants also traverse the Official Notice taken by the Examiner because the Official Notice is “unsupported by documentary evidence.” “The applicant should be presented with the **explicit basis** on which the examiner regards the matter as subject to official notice **and be allowed to challenge** the assertion” *See* M.P.E.P. § 2144.03(B). (Emphasis added). In the Office Action, the Examiner merely stated the Official Notice but provided no basis at all for the Official Notice. Thus, Appellants were not allowed the opportunity to challenge the Official Notice because the

Examiner provided no line of reasoning in support of the Official Notice which Appellants could challenge.

Accordingly, the combination of Moskowitz, Shur, and Examiner Official Notice does not teach or suggest each and every feature of claim 8. “All words in a claim must be considered in judging the patentability of that claim against the prior art.” M.P.E.P. § 2143.03. To establish a *prima facie* case of obviousness, “the prior art reference (or references when combined) must teach or suggest all the claim limitations.” M.P.E.P. § 2142. Accordingly, the Examiner has failed to establish a *prima facie* case of obviousness regarding claim 8.

Claim 18 recites similar features as claim 8 and is rejected along the same rationale. Claims 9 and 19 depend respectively from claims 8 and 18. Accordingly, the Examiner has also failed to establish a *prima facie* case of obviousness regarding claims 9, 18, and 19.

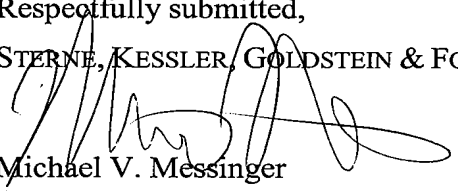
The rejection of claims 8, 9, 18, and 19 must be reversed.

VIII. Conclusion

Claims 1-25 are patentable over the cited art. Therefore, Appellants respectfully request that the Board reverse the Examiner's final rejection of these claims under 35 U.S.C. §103 and remand this application for issue.

Respectfully submitted,

STERNE, KESSLER, GOLDSTEIN & FOX P.L.L.C.



Michael V. Messinger
Attorney for Appellants
Registration No. 37,575

Date: May 5, 2009
1100 New York Avenue, N.W.
Washington, D.C. 20005-3934
(202) 371-2600

IX. Claims Appendix

1. (Previously Presented) A method for providing secure transmissions across a network comprising a client device and a server, the method comprising:

at the client device, generating a stream of watermark bits;

generating a plurality of watermarks, each of the plurality of watermarks comprising a respective index number and a respective portion of the stream of watermark bits;

inserting the plurality of watermarks into respective headers of a plurality of outgoing packets;

receiving, at the server, the plurality of outgoing packets; and

determining if a received packet is valid based on the watermark in the header of the received packet.

2. (Previously Presented) The method of claim 1, wherein generating the stream of watermark bits includes generating a stream of watermark bits from an authorization and synchronization packet previously exchanged between the client device and the server.

3. (Previously Presented) The method of claim 1, further comprising activating a session by exchanging an authorization and synchronization packet between the client device and the server.

4. (Original) The method of claim 1, further comprising:

discarding the packet, if the watermark is not valid.

5. (Original) The method of claim 1, wherein determining if a received packet is valid comprises:

comparing the watermark of the received packet to a first and a second window, each of the windows comprising a set of expected watermarks; and

accepting the watermark as valid if the received watermark matches one of the expected watermarks in the first or second windows.

6. (Previously Presented) The method of claim 5, wherein the set of expected watermarks are generated from an authorization and synchronization packet previously exchanged between the client device and the server.

7. (Previously Presented) The method of claim 5, comprising:

discarding the packet, if the watermark does not match one of the expected watermarks in the first or second windows.

8. (Previously Presented) The method of claim 5, wherein comparing the watermark further comprises:

maintaining at the server a record of a pivotal index number representing the index number of the highest-numbered valid watermark received from the client device; and

comparing the watermark of the received packet to a first and a second window, each of the windows comprising a set of expected watermarks and wherein

the first window represents expected watermarks whose index numbers precede the pivotal index number and the second window represents expected watermarks whose index numbers immediately supersede the pivotal index number.

9. (Original) The method of claim 8, comprising:

increasing the pivotal index number if a match is found in the second window and deleting the matching expected watermark from the second window.

10. (Original) The method of claim 1, wherein the stream of watermark bits is generated by a stream cipher.

11. (Original) The method of claim 1, wherein inserting at least one of the plurality of watermarks includes determining whether a valid session exists and inserting the at least one of the plurality of watermarks only if the valid session exists.

12. (Previously Presented) A system for providing secure transmissions across a network, the system comprising:

a client device for

generating a stream of watermark bits;

generating a plurality of watermarks, each of the plurality of watermarks comprising a respective index number and a respective portion of the stream of watermark bits;

inserting the plurality of watermarks into respective headers of a plurality of outgoing packets; and

transmitting the outgoing packets to a server; and
a server for
receiving the plurality of outgoing packets; and
determining if a received packet is valid based on the watermark in the
header of the received packet.

13. (Previously Presented) The system of claim 12, wherein the stream of watermark bits are generated from an authorization and synchronization packet previously exchanged between the client device and the server.

14. (Original) The system of claim 12, wherein inserting at least one of the plurality of watermarks includes determining whether a valid session exists and inserting the at least one of the plurality of watermarks only if the valid session exists.

15. (Previously Presented) The system of claim 12, wherein the server further discards the packet, if the watermark is not valid.

16. (Previously Presented) The system of claim 12, wherein the server further determines if a received packet is valid by comparing the watermark of the received packet to a first and a second window, each of the windows comprising a set of expected watermarks; and

accepting the received watermark as valid if the received watermark matches one of the expected watermarks in the first or second windows.

17. (Previously Presented) The system of claim 16, wherein the server further discards the packet, if the received watermark does not match any expected watermarks in the first or second windows.

18. (Previously Presented) The system of claim 16, wherein comparing the watermark further comprises:

maintaining at the server a record of a pivotal index number representing the index number of the highest-numbered valid watermark received from the client device; and

comparing the watermark of the received packet to a first and a second window, each of the windows comprising a set of expected watermarks and wherein the first window represents expected watermarks whose index numbers precede the pivotal index number and the second window represents expected watermarks whose index numbers immediately supersede the pivotal index number.

19. (Previously Presented) The system of claim 18, wherein the server increases the pivotal index number if a match is found in the second window and deletes the matching expected watermark from the second window.

20. (Previously Presented) The system of claim 12, wherein the stream of watermark bits is generated by a stream cipher.

21. (Previously Presented) A system for providing secure transmissions across a network from a client device to a server, the system comprising:

means for generating a stream of watermark bits;

means for generating a plurality of watermarks, each of the plurality of watermarks comprising a respective index number and a respective portion of the stream of watermark bits;

means for inserting the plurality of watermarks into respective headers of a plurality of outgoing packets; and

means for transmitting the outgoing packets to a server capable of determining if a received packet is valid based on the watermark in the header of the received packet.

22. (Previously Presented) The method of claim 1, wherein each of the plurality of watermarks comprises a different respective index number and a different respective portion of the stream of watermark bits.

23. (Previously Presented) The method of claim 1, wherein each of the plurality of watermarks comprises a different respective index number and a respective portion of the stream of watermark bits.

24. (Previously Presented) The system of claim 12, wherein each of the plurality of watermarks comprises a different respective index number and a different respective portion of the stream of watermark bits.

25. (Previously Presented) The system of claim 12, wherein each of the plurality of watermarks comprises a different respective index number and a respective portion of the stream of watermark bits.

X. Evidence Appendix

Not applicable.

XI. Related Proceedings Appendix

Not applicable.